Algebraische Zahlentheorie: [MTH-1483]

Ilia Pirashvili

Arbeitsblatt 12

1 Allgemeine Hinweise

Maximale Punktzahl die man in diesem Arbeitsblatt erwerben kann sind 10 Punkte. Aufgaben können frei gewählt werden.

Lösungen werden nächste Woche (Donnerstag) sowohl elektronisch (als PDF) bereitgestellt, wie auch in der Vorlesungszeit (12:15 – 13:45) live/online von mir via Zoom erklärt.

Bei Unverständnissen, Fragen oder wenn Ihr Fehler findet, bitte an
ilia.pirashvili@math.uni-augsburg.de
wenden.

Die Punkte der Arbeitsblätter werden in die Endnote eingehen! Abgabefirst ist bis einschließlich Mittwoch (22/07) (da nächste Woche keine Aufgaben sein werden). Viel Glück und viel Erfolg.

2 Aufgaben

Aufgabe 1 (1 Punkt). Sei $f : R \to S$ ein Ringhomomorphismus. Man erinnere sich, dass wenn $\mathfrak{p}$ ein Primideal von S ist, $f^{-1}(\mathfrak{p})$ ein Primideal von R ist. Sei K ein algebraisches Zahlenkörper und $0 \neq \mathfrak{p}$ ein Primideal von $\mathfrak{o}_K$. Beweise, dass es einen eindeutigen Primzahl $p \in \mathbb{Z}$ gibt, mit $p \in \mathfrak{p}$.

Lösung. Sieh unsere Diskussion in *Norm von Primidealen*. Das einzige, was noch zu zeigen verbleibt ist, dass $p \neq (0)$. Da die Norm eines Ideals immer im Ideal drin ist, und $\mathsf{N}(I) = 0 \Leftrightarrow I = 0$, folgt, dass $(p) \neq 0$ ist. □

Aufgabe 2 (3 Punkte). Sei $K = \mathbb{Q}(\sqrt{11})$. Sind folgende Ideale Maximalideale von $\mathfrak{o}_K = \mathbb{Z}[\sqrt{11}]$?

i) (1 Teilpunkt) $(3) \subseteq \mathfrak{o}_K$,

ii) (1 Teilpunkt) $(5) \subseteq \mathfrak{o}_K$,

ii) (1 Teilpunkt) $(7) \subseteq \mathfrak{o}_K$.

Lösung. Wir wissen von Dedekinds Primfaktorzerlegungssatz, dass (p) als $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ faktorisiert. Da $(p) \subseteq \mathfrak{p}_i$ folgt, ist (p) genau dann Maximal, wenn $r = 1$ und $e_1 = 1$. Daher, genau dann, wenn das Minimalpolynom $\mathfrak{m}_\alpha = x^2 - 11$ von $\alpha = \sqrt{11}$ irreduzibel ist modulo der gegebenen Primzahl.

Da dies eine quadratische Gleichung ist, brauchen wir nur überprüfen, ob $\mathfrak{m}_\alpha$ eine Wurzel hat, modulo der gegebenen Primzahl. Also, ob $\mathfrak{m}_\alpha(x)$ ein viel faches von p ist, für $-\frac{p-1}{2} \leq x \leq \frac{p-1}{2}$.

Wir lösen alle 3 Fälle zusammen, da beim Lösen von $p = 7$ die andern mit gelöst werden.

$x =$	$\mathfrak{m}_\alpha(x) =$
0	-11
± 1	$-10 = -2 \cdot 5$
± 2	-7
± 3	-2

Wir können direkt sehen, dass $(5), (7)$ keine Maximalideale sind, aber (3) ein Maximalideal ist.

(Zur Erläuterung, da z. B. 5 vorkommt, ist $\mathfrak{m}_\alpha$ modulo 5 reduzibel, da $\mathfrak{m}_\alpha(1) = -10 \equiv 0 \mod 5$. Daher ist $\mathfrak{m}_\alpha \equiv (x-1)(x+1) \mod 5$ und als solches haben wir $(5) = (5, \sqrt{-11}-1)(5, \sqrt{-11}+1)$. 3 kommt nicht vor, daher ist $\mathfrak{m}_\alpha$ irreduzibel modulo 3). □

Aufgabe 3 (3 Punkte). Sei $K = \mathbb{Q}(\sqrt{3})$. Faktorisiere folgende Ideale in $\mathfrak{o}_K = \mathbb{Z}[\sqrt{3}]$ als Produkt von Maximalidealen:

i) (1 Teilpunkt) $(3) \subseteq \mathfrak{o}_K$,

ii) (1 Teilpunkt) $(5) \subseteq \mathfrak{o}_K$,

iii) (1 Teilpunkt) $(7) \subseteq \mathfrak{o}_K$.

Lösung. Dies kann man direkt mit Dedekinds Primfaktorzerlegungssatz machen. Das Minimalpolynom ist $\mathfrak{m}_\alpha = x^2 - 3$. Wir zerlegen es nun modulo $3, 5$ und 7. Dazu erstellen wir die folgende Tabelle:

x	$\mathfrak{m}_\alpha(x)$		$\mathfrak{m}_\alpha \equiv$	mod p
0	-3		x^2	mod 3
± 1	-2	was uns volgende Zerlegung liefert	$x^2 - 3$	mod 5
± 2	1		$x^2 - 3$	mod 7
± 3	$6 = 2 \cdot 3$			

Daher können wir alle der Hauptideale wie folgt zerlegen:

i) $(3) = (3, \sqrt{-3})^2 = (\sqrt{-3})^2$

ii) (5) ist ein Maximalideal.

iii) (7) ist ein Maximalideal.

□

Aufgabe 4 (2 Punkte). Sei $K = \mathbb{Q}(\sqrt{-6})$. Faktorisiere $(10) \subseteq \mathfrak{o}_K = \mathbb{Z}[\sqrt{-6}]$ als Produkt von Maximalidealen.

Lösung.

x	$\mathfrak{m}_\alpha(x)$
0	$6 = 2 \cdot 3$
± 1	7
± 2	$10 = 2 \cdot 5$
± 3	$15 = 3 \cdot 5$

Als erstes berechnen wir die Norm von $I = (10)$. Wir wissen, dass $\mathsf{N}((10)) = |\mathsf{N}(10)| = 10^{[K:\mathbb{Q}]} = 100$. Dann zerlegen wir 100 in Primzahlen, was uns $100 = 2^2 \cdot 5^2$ liefert. Als ersten Schritt suchen wir also Maximalideale mit der gegebenen Norm.

Sei $\mathfrak{p}$ ein Maximalideal mit Norm 5. Dann muss $5 = \mathsf{N}(\mathfrak{p}) \in \mathfrak{p}$ gelten. Als solches haben wir $\mathfrak{p} \mid (5)$. Wir müssen also (5) in Maximalideale zerlegen. Ähnlich müssen wir (2) in Maximalideale zerlegen.

Dazu betrachten wir unsere Tabelle, was besagt, dass

$$(2) = \mathfrak{p}_2^2 = (2, \sqrt{-6})^2$$

und

$$(5) = \mathfrak{p}_5\mathfrak{q}_5 = (5, \sqrt{-6}-2)(5, \sqrt{-6}+2).$$

Als solches müssen wir $A = \mathfrak{p}_2^2\mathfrak{p}_5^2, B = \mathfrak{p}_2^2\mathfrak{p}_5\mathfrak{q}_5$ und $C = \mathfrak{p}_2^2\mathfrak{q}_5^2$ untersuchen. Genau eines von denen wird mit (10) übereinstimmen.

In diesem Fall ist es trivial zu sehen, dass es $B = \mathfrak{p}_2^2\mathfrak{p}_5\mathfrak{q}_5$ sein muss, da $\mathfrak{p}_2^2 = (2)$ und $\mathfrak{p}_5\mathfrak{q}_5 = (5)$ gilt. Daher ist $B = \mathfrak{p}_2^2\mathfrak{p}_5\mathfrak{q}_5 = (2)(5) = (10)$. □

Aufgabe 5 (4 Punkte). Sei $K = \mathbb{Q}(\sqrt[3]{3})$. Faktorisiere folgende Ideale als Produkt von Maximalidealen:

i) (2 Teilpunkte) $(3) \subseteq \mathfrak{o}_K = \mathbb{Z}[\sqrt[3]{3}]$

ii) (2 Teilpunkte) $(10) \subseteq \mathfrak{o}_K = \mathbb{Z}[\sqrt[3]{3}]$

Lösung. Wir erstellen wieder die Wertetabelle, da wir bald die Faktorisierung von $\mathfrak{m}_\alpha = x^3 - 3$ modulo $2, 3$ und 5 brauchen werden. (In diesem Fall ist dies einfach zu sehen, da die Norm der Ideale Potenzen von $2, 3, 5$ sein müssen). Wir haben

x	$\mathfrak{m}_\alpha(x)$
-2	-11
-1	$-4 = -2^2$
0	-3
1	-2
2	5

i) Bei Dedekind haben wir $(3) = \mathfrak{p}_3^3 = (3, \sqrt[3]{3})^3$.

ii) Wir haben $\mathsf{N}((10)) = |\mathsf{N}(10)| = 10^{[K:\mathbb{Q}]} = 1000 = 2^3 \cdot 5^3$. Von der Tabelle wissen wir, dass $-1 \equiv 1 \mod 2$ eine Wurzel von $\mathfrak{m}_\alpha$ modulo 2 ist. Daher gilt $(x-1) \mid (x^3 - 3) \mod 2$. Wir führen die schriftliche Division $x^3 - 3 : (x-1)$ durch und erhalten

$$x^3 - 3 = (x-1)(x^2 + x + 1) - 2 \equiv (x-1)(x^2 + x + 1) \mod 2$$

.

Da die einzige Wurzel von $\mathfrak{m}_\alpha$ modulo 2 nur 1 sein kann (siehe Tabelle), brauchen wir nur $x^2 + x + 1$ nur darauf untersuchen. Wir haben $(x^2 + x + 1)(1) = 3 \equiv 1 \mod 2 \not\equiv 0 \mod 2$, woraus wir schließen können, dass $x^2 + x + 1$ irreduzibel ist modulo 2.

Bei Dedekind haben wir also

$$(2) = \mathfrak{p}_2\mathfrak{q}_2 = (2, \sqrt[3]{3} - 1)(2, \sqrt[3]{3}^2 + \sqrt[3]{3} + 1).$$

Die Tabelle sagt auch, dass $(x-2) \mid x^3 - 3 \mod 5$. Schriftliche Division besagt

$$x^3 - 3 = (x-2)(x^2 + 2x + 4) + 5 \equiv (x-2)(x^2 + 2x + 4) \mod 5.$$

Da 5 nur bei $x = 2$ als Teiler von $\mathfrak{m}_\alpha(x)$ vorkommt, kann nur 2 eine Wurzel von $x^2 + 2x + 4$ sein. Wir haben

$$(x^2 + 2x + 4)(2) = 4 + 4 + 4 = 12 \not\equiv 0 \mod 5.$$

Daher ist $x^2 + 2x + 4$ irreduzibel modulo 5. Dedekind besagt nun

$$(5) = \mathfrak{p}_5\mathfrak{q}_5 = (5, \sqrt[3]{3} - 2)(5, \sqrt[3]{3}^2 + 2\sqrt[3]{3} + 4).$$

Rein von der Norm kann jedes der Ideale

$$\mathfrak{p}_2^3\mathfrak{p}_5^3, \mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{q}_5, \mathfrak{p}_2\mathfrak{q}_2\mathfrak{p}_5^3 \quad \text{und} \quad \mathfrak{p}_2\mathfrak{q}_2\mathfrak{p}_5\mathfrak{q}_5$$

gleich (10) sein. Da jedoch

$$\mathfrak{p}_2\mathfrak{q}_2\mathfrak{p}_5\mathfrak{q}_5 = (2)(5) = (10)$$

gilt, haben wir die Lösung schon gefunden.

□

Aufgabe 6 (4 Punkte). Sei $d \not\equiv 1 \mod 4$ eine quadratfreie Zahl und p eine Primzahl, so dass $d \equiv a^2 \mod p$. Sein $\mathfrak{p} := (p, a + \sqrt{d}), \mathfrak{q} := (p, a - \sqrt{d}) \subseteq \mathbb{Z}[\sqrt{d}]$.

i) (1 Teilpunkt) Beweise, dass $\mathfrak{p}$ und $\mathfrak{q}$ Primideale sind.

ii) (1 Teilpunkt) Zeige, dass $\mathsf{N}(\mathfrak{p}) = \mathsf{N}(\mathfrak{q}) = p$.

iii) (1 Teilpunkt) Beweise, dass $(p) = \mathfrak{p}\mathfrak{q}$.

iv) (1 Teilpunkt) Zeige, dass $\mathfrak{p} = \mathfrak{q}$ genau dann, wenn $p \mid 2d$.

Lösung. Wir haben $\mathbb{Z}[\sqrt{d}] = \mathfrak{o}_K$, wobei $K = \mathbb{Q}(\sqrt{d})$, da $d \not\equiv 1 \mod 4$. Daher ist das Minimalpolynom der Erweiterung $\mathfrak{m}_\alpha = x^2 - d$.

i) Da $d \equiv a^2 \mod p$ haben wir

$$\mathfrak{m}_\alpha(\pm a) = (\pm a)^2 - d \equiv a^2 - a^2 \mod p = 0 \mod p.$$

Als solches sind a und $-a$ Wurzeln von $\mathfrak{m}_\alpha \mod p$ und wir haben

$$\mathfrak{m}_\alpha = x^2 - d \equiv (x - a)(x + a) \mod p.$$

Laut Dedekind sind also

$$\mathfrak{p} = (p, a + \sqrt{d}) \quad \text{und} \quad \mathfrak{q} = (p, a - \sqrt{d})$$

Maximalideale.

ii) Laut Dedekind wissen wir, dass $\mathsf{N}(\mathfrak{p}) = p^{\mathsf{grad}(x-d)} = p$. Ebenso für $\mathfrak{q}$.

iii) Auch dies ist schlicht und einfach eine Konsequenz von Dedekinds Primfaktorzerlegungssatz.

iv) Wir müssen die Implikation auf beiden Seiten zeigen.

$\Rightarrow$: Sei $\mathfrak{p} = \mathfrak{q}$. Dann ist $a - \sqrt{d} \in \mathfrak{p}$. Daher ist

$$\begin{aligned}
& a + \sqrt{d} - (a - \sqrt{d}) = 2\sqrt{d} \in \mathfrak{p} \\
\Rightarrow\ & (2\sqrt{d}) \subseteq \mathfrak{p} \\
\Rightarrow\ & \mathfrak{p} \mid (2\sqrt{d}) \\
\Rightarrow\ & \mathsf{N}(\mathfrak{p}) \mid \mathsf{N}((2\sqrt{d})) \quad \text{da die Norm multiplikativ ist} \\
\Rightarrow\ & p \mid |\mathsf{N}(2\sqrt{d})| = |4d| \\
\Rightarrow\ & p \mid 2d, \quad \text{da } p \text{ eine Primzahl is.}
\end{aligned}$$

$\Leftarrow$: Auf der anderen Seite, sei $p \mid 2d$. Dann gilt $p \mid 2$ oder $p \mid d$, da p eine Primzahl ist. (Es kann auch beides sein, wenn d selber gerade ist, aber eines der zwei Annahmen muss gelten). Wir haben also zwei Fälle anzusehen:

Fall 1: Sei $p \mid d$. Dann ist $\mathfrak{m}_\alpha = x^2 - d \equiv x^2 \mod p$. Dann ist $i = 1, f_1 = x$ und $e_1 = 2$, in der Notation von Dedekinds Primfaktorzerlegungssatz. Als solches gilt $(p) = (2, \sqrt{d})^2$ und $\mathfrak{p} = (2, \sqrt{d}) = \mathfrak{q}$, da es eine eindeutige Zerlegung in Maximalidealen gibt.

Fall 2: Sei $p \mid 2$. Dann ist die Zerlegung von Teil i)

$$\mathfrak{m}_\alpha = x^2 - d \equiv (x - a)(x + a) \mod p$$

äquivalent zu

$$\mathfrak{m}_\alpha = x^2 - d \equiv (x - a)(x - a) \mod 2 = (x - a)^2 \mod 2,$$

wobei $a \in \{0, 1\}$. Daher gilt

$$(p) = (2, a - \sqrt{d})^2$$

woraus $(\mathfrak{p}) = (2, a - \sqrt{d}) = \mathfrak{q}$ folgt.

□

Sei $f : R \to S$ ein Ringhomomorphismus und $I \subseteq R$ ein Ideal. Dann bezeichnen wir mit I_S, dass Ideal (in S) erzeugt mit $f(I)$. Wenn f eine Einbettung ist, gilt $I_S = (is), i \in I, s \in S$, also das Ideal erzeugt mit allen Produkten is. Folgendes gilt im solchem Fall:

- $(IJ)_S = I_S J_S$
- $(I^n)_S = (I_S)^n$ und
- $(a)_L = (a)$ (wobei wir a in der rechten Seite als ein Element von S auffassen. Anders gesagt, Hauptideale bleiben Hauptideale und werden vom selben Element erzeugt).

Aufgabe 7 (3). Sei $K = \mathbb{Q}(\sqrt{-13})$ und $I = (2, 1 + \sqrt{-13}) \subseteq \mathfrak{o}_K$.

i) (1 Teilpunkt) Beweise, dass $I^2 = (2)$.

ii) (1 Teilpunkt) Zeige, dass I kein Hauptideal ist.

iii) (1 Teilpunkt) Sei $L = \mathbb{Q}(\sqrt{-13}, \sqrt{2})$. Zeige, dass $I_{\mathfrak{o}_L} = (\sqrt{2}) \subseteq \mathfrak{o}_L$. - *Hierzu sagt man, dass man ein Ideal durch eine Erweiterung zu einem Hauptideal gemacht hat.*

Lösung. i) Wir haben

$$\begin{aligned} I^2 &= (2, 1 + \sqrt{-13})^2 \\ &= (4, 2(1 + \sqrt{-13}), 2\sqrt{-13} - 12) \\ &= (2)(2, 1 + \sqrt{-13}, \sqrt{-13} - 6) \\ &= (2)(1) \\ &= (2) \end{aligned}$$

Um die vorletzte Gleichung zu sehen, bemerken wir, dass aus $2, \sqrt{-13} - 6 \in J \Rightarrow \sqrt{-13} \in J$. Aus $\sqrt{-13}, 1 + \sqrt{-13} \in J \Rightarrow 1 \in J$.

ii) Da $I^2 = (2)$ wissen wir, dass

$$\mathsf{N}(I)^2 = \mathsf{N}(I^2) = \mathsf{N}((2)) = |\mathsf{N}(2)| = 2^{[K:\mathbb{Q}]} = 4.$$

Daher ist

$$\mathsf{N}(I) = 2.$$

Sei $I = \alpha = a + b\sqrt{-13}$. Dann muss $|\mathsf{N}(\alpha)| = 2$ sein. Also muss $a^2 + 13b^2 = 2$ gelten, was nicht möglich ist. (b muss 0 sein, da sonst $a^2 + 13b^2 \geq 13$ und $a^2 = 2$ hat keine Lösung über $\mathbb{Q}$).

iii) Wir haben $L = \mathbb{Q}(\sqrt{-13}, \mathsf{q}2) = \mathbb{Q}(\sqrt{-13} + \sqrt{2})$. Sei $\theta = \sqrt{-13} + \sqrt{2}$. Dann ist

$$\theta^2 = (\sqrt{-13} + \sqrt{2})^2 = -11 + \sqrt{-26}$$

woraus

$$(\theta^2 + 11)^2 = \theta^4 + 22\theta^2 + 121 = -26.$$

Also ist

$$\mathfrak{m}_\theta = x^4 + 22x^2 + 137$$

das Minimalpolynom der primitiven Elements θ. Wir wollen nun $(2) \subseteq L$ faktorisieren. Dazu faktorisieren wir $\mathfrak{m}_\theta$ modulo 2. Wir haben

$$\mathfrak{m}_\theta \equiv x^4 + 1 \mod 2.$$

Es ist direkt klar, dass 1 eine Wurzel davon ist (modulo 2). Wir haben

$$x^4 + 1 \equiv (x - 1)(x^3 + x^2 + x + 1) \mod 2.$$

$x^3 + x^2 + x + 1$ hat selber die 1 als Wurzel, darum faktorisieren wir weiter zu

$$x^4 + 1 \equiv (x-1)^2(x^2+1).$$

Wir können weiter machen zu

$$x^4 + 1 \equiv (x-1)^4.$$

Daher gilt laut Dedekind

$$(2) = \mathfrak{p}_2^4, \quad \text{wobei} \quad \mathfrak{p}_2 = (2, \theta - 1).$$

Nun sehen wir uns die Normen von $(2, 1+\sqrt{-13}) \subseteq L$ und $(\sqrt{2}) \subseteq L$ an. Es gilt

$$\mathsf{N}((2, 1+\sqrt{-13})^2) = \mathsf{N}((2)) = |\mathsf{N}(2)| = 2^{[L:\mathbb{Q}]} = 16.$$

Daher ist $\mathsf{N}((2, 1+\sqrt{-13})) = 4$, was

$$L \supseteq (2, 1+\sqrt{-13}) = \mathfrak{p}_2^2$$

impliziert. Auf der andern Seite ist

$$\mathsf{N}((\sqrt{2})^2) = \mathsf{N}((2)) = 16,$$

also ist

$$\mathsf{N}((\sqrt{2})) = 4,$$

was ebenso

$$L \supseteq (\sqrt{2}) = \mathfrak{p}_2^2$$

ergibt. Daher haben diese die selbe Zerlegung, also müssen die Ideale miteinander übereinstimmen.

Man erinnere sich, dass $I = J$ wenn $I \subseteq J$ und $\mathsf{N}(I) = \mathsf{N}(J)$. Daher würde es hier ausreichen, eine Inklusion $(\sqrt{2}) \subseteq (2, 1+\sqrt{-13})$ oder umgekehrt zu zeigen. Dies scheint jedoch nicht so einfach zu sein.

□

Aufgabe 8 (3 Punkte). Sei $d \equiv 1 \mod 4$ und quadratfrei mit $d \neq 1$. Beweise, dass $\mathbb{Z}[\sqrt{d}]$ kein Hauptidealring ist.

Hinweis: Faktorisiere $d-1$. Hinweis 2: Wir haben einen Element $r \in R$ prim genannt, wenn $(p) \subseteq R$ ein Primideal war. Was wissen wir über irreduzible und prim Elemente in einem Hauptidealbereich?

Lösung. Wir benutzen [Vorlesung ??, Proposition ??.]. Hier wurde gezeigt, dass in einem Hauptidealring jedes irreduzible Element prim ist.

Wir haben $d \equiv 1 \mod 4$. Daher, $d - 1 = 4n$, für irgendein $n \in \mathbb{N}$. Auf der anderen Seite gilt $d - 1 = (\sqrt{d}-1)(\sqrt{d}+1)$. Zusammengefasst ergibt es

$$4n = (\sqrt{d}-1)(\sqrt{d}+1).$$

Wir behaupten, dass $2 \in \mathbb{Z}[\sqrt{d}]$ irreduzibel-, aber $(2) \subseteq \mathbb{Z}[\sqrt{d}]$ nicht prim ist.

Um zu sehen, dass $2 \in \mathbb{Z}[\sqrt{d}]$ irreduzibel ist, sei $xy = 2, x, y \in \mathbb{Z}[\sqrt{d}]$. Wir bemerken wir, dass $\mathsf{N}(2) = 4$ ist. Daher muss $\mathsf{N}(x) = 2 = \mathsf{N}(y)$ damit weder x noch y eine Einheit ist. Sei also

$$\mathsf{N}(a + b\sqrt{d}) = a^2 - b^2 d = 2.$$

Da $d \equiv 1 \mod 4$ muss

$$a^2 - b^2 d \equiv a^2 - b^2 \mod 4,$$

was uns

$$a^2 - b^2 \equiv 2 \mod 4,$$

also

$$(a-b)(a+b) \equiv 2 \mod$$

liefert. Wir behaupten, dass dies nicht möglich ist. Man betrachte sich die Multiplikationstabelle in $\mathbb{Z}/4\mathbb{Z}$:

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Wir haben also 4 Fälle:

F1:

$$\left.\begin{matrix}(a-b) = 1 \mod 4\\ (a+b) = 2 \mod 4\end{matrix}\right\} \Rightarrow \left.\begin{matrix}(a-b) = 1 \mod 2\\ (a+b) = 0 \mod 2\end{matrix}\right\} \Rightarrow \left.\begin{matrix}(a+b) = 1 \mod 2\\ (a+b) = 0 \mod 2\end{matrix}\right\} \Rightarrow 0 = 1 \text{ in } \mathbb{Z}/2\mathbb{Z}. \text{ Widerspruch.}$$

F2:

$$\left.\begin{matrix}(a-b) = 2 \mod 4\\ (a+b) = 1 \mod 4\end{matrix}\right\} \Rightarrow \left.\begin{matrix}(a-b) = 2 \mod 2\\ (a+b) = 1 \mod 2\end{matrix}\right\} \Rightarrow \left.\begin{matrix}(a+b) = 0 \mod 2\\ (a+b) = 1 \mod 2\end{matrix}\right\} \Rightarrow 0 = 1 \text{ in } \mathbb{Z}/2\mathbb{Z}. \text{ Widerspruch.}$$

F3:

$$\left.\begin{matrix}(a-b) = 3 \mod 4\\ (a+b) = 2 \mod 4\end{matrix}\right\} \Rightarrow \left.\begin{matrix}(a-b) = 1 \mod 2\\ (a+b) = 0 \mod 2\end{matrix}\right\} \Rightarrow \left.\begin{matrix}(a+b) = 1 \mod 2\\ (a+b) = 0 \mod 2\end{matrix}\right\} \Rightarrow 0 = 1 \text{ in } \mathbb{Z}/2\mathbb{Z}. \text{ Widerspruch.}$$

F4:

$$\left.\begin{matrix}(a-b) = 2 \mod 4\\ (a+b) = 3 \mod 4\end{matrix}\right\} \Rightarrow \left.\begin{matrix}(a-b) = 0 \mod 2\\ (a+b) = 1 \mod 2\end{matrix}\right\} \Rightarrow \left.\begin{matrix}(a+b) = 0 \mod 2\\ (a+b) = 1 \mod 2\end{matrix}\right\} \Rightarrow 0 = 1 \text{ in } \mathbb{Z}/2\mathbb{Z}. \text{ Widerspruch.}$$

Daher ist $2 \in \mathbb{Z}[\sqrt{d}]$ irreduzibel.

Auf der anderen Seite ist $(\sqrt{d}-1)(\sqrt{d}+1) \in (2)$, da es ja gleich $4n$ war. Wir behaupten, dass keines der beiden Multiplikanden ein Vielfaches von 2 ist, also die nicht in (2) liegen.

Sei nämlich $2(a+b\sqrt{d}) = (\sqrt{d} \pm 1)$. Dann ist

$$2a + 2b\sqrt{d} = \sqrt{d} \pm 1,$$

also

$$2a = \pm 1$$

was ein Widerspruch ist. □

Aufgabe 9 (2 Punkt). Sei $K = \mathbb{Q}(\sqrt{-6})$. Finde alle Ideale der Norm $4, 10$ und 15.

Lösung. Wir wissen, dass jedes Ideal ein Produkt von Maximalidealen ist (und dies eindeutig). Daher um Ideale der Norm n zu finden, müssen wir Maximalideale finden, dessen Norm n teilen. Die Norm eines Maximalideals ist eine Potenz einer Primzahl. Also, $\mathsf{N}(\mathfrak{p}) = p^r$. Da aber $\mathsf{N}(\mathfrak{p}) = p^r \in \mathfrak{p}$ und $\mathfrak{p}$ ein Maximalideal ist, folgt, dass $p \in \mathfrak{p}$ sein muss. Daraus wiederum folgt, dass $\mathfrak{p} \mid (p)$.

In anderen Worten, um Ideale der Norm n zu finden, faktorisieren wir n in Primzahlen als

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

und faktorisieren dann die Hauptideale (p_i) als Produkt von Maximalidealen. Dann nehmen wir jede Kombination der Maximalideale, welche die gewünschte Norm ergeben.

$\mathsf{N} = 4$. Wir haben $4 = 2^2$, daher faktorisieren wir (2) mit Dedekinds Primfaktorzerlegungssatz. Das Minimalpolynom $\mathfrak{m}_{\sqrt{-6}} = x^2 + 6$ modulo 2 ist x^2, was natürlich reduzibel ist. Daher ist

$$(2) = \mathfrak{p}_2^2 = (2, \sqrt{-6})^2.$$

Es folgt, dass (2) das einzige Ideal ist mit Norm 4 ist.

$\mathsf{N} = 10$. Wir haben $(10) = 2 \cdot 5$. Wir faktorisieren also die Ideale (2) und (5). $(2) = \mathfrak{p}_2^2$, wie schon oben gezeigt und da

$$\mathfrak{m}_{\sqrt{-6}} \equiv x^2 + 1 \equiv x^2 - 4 \equiv (x+2)(x-2) \mod 5,$$

folgt, dass

$$(5) = \mathfrak{p}_5\mathfrak{q}_5 = (5, \sqrt{-6} - 2)(5, \sqrt{-6} + 2).$$

Daher sind

$$\mathfrak{p}_2\mathfrak{p}_5 = (2, \sqrt{-6})(5, \sqrt{-6} - 2)$$

und

$$\mathfrak{p}_2\mathfrak{q}_5 = (2, \sqrt{-6})(5, \sqrt{-6}22)$$

alle Ideale der Norm 10.

$\mathsf{N} = 15$. Da wir uns (5) schon angesehen haben, faktorisieren wir nun noch (3). Es gilt

$$\mathfrak{m}_{\sqrt{-6}} \equiv x^2 \mod 3,$$

was uns

$$(3) = \mathfrak{p}_3^2 = (3, \sqrt{-6})^2.$$

Daher sind die einzigen Ideale der Norm 15 gleich

$$\mathfrak{p}_3\mathfrak{p}_5 = (3, \sqrt{-6})(5, \sqrt{-6} - 2)$$

und

$$\mathfrak{p}_3\mathfrak{q}_5 = (3, \sqrt{-6})(5, \sqrt{-6} + 2).$$

□

Aufgabe 10 (1 Punkt). Sei $K = \mathbb{Q}(\sqrt{-2})$. Bestimme die Klassgruppe $\mathrm{Cl}(\mathfrak{o}_K)$.

Lösung. Wir erinnern uns an die Minkowskis Konstante

$$c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{o}_K)|}.$$

Wir wissen, dass jedes Element in $\mathrm{Cl}(\mathfrak{o}_K) = \mathcal{I}_K^*/\mathcal{P}_K^*$ einen Repräsentanten Ideal mit Norm weniger als c hat.

Als erstes berechnen wir die Diskriminante $\Delta(\mathfrak{o}_K)$. Es gilt

$$\Delta(\mathfrak{o}_K) = \det \begin{pmatrix} 1 & \sqrt{-2} \\ 1 & -\sqrt{-2} \end{pmatrix}^2 = (-2\sqrt{-2})^2 = 8.$$

Daher ist

$$\sqrt{|\Delta(\mathfrak{o}_K)|} = 2\sqrt{-2}.$$

Es ist offensichtlich, dass $s = 1$, da $\sqrt{-2} \in \mathbb{C} \setminus \mathbb{R}$. Daher ist

$$c = \left(\frac{2}{\pi}\right)^s \sqrt{\Delta} < 2.$$

Als solches $\mathrm{Cl}(\mathfrak{o}_K)$ nur einen Element haben, die Einheit, was uns

$$\mathrm{Cl}(\mathfrak{o}_K) = 1,$$

die triviale Gruppe, gibt. □

Aufgabe 11 (2 Punkte). Sei $K = \mathbb{Q}(\alpha)$ mit $\mathfrak{o}_K = \mathbb{Z}[\alpha]$, so dass für jeden Primzahl $p \leq c$, wobei c die Minkowski Konstante ist, jedes Maximalideal in der Zerlegung von (p) ein Hauptideal ist.

Beweise, dass $\mathrm{Cl}(\mathfrak{o}_K) = 1$ ist. Also, dass K ein Hauptidealring ist.

Lösung. Wir wissen, jedes Element in $\mathrm{Cl}(\mathfrak{o}_K)$, was bei Definition eine Äquivalenzklasse von Idealen ist, einen Repräsentanten Ideal I mit Norm kleiner als c, die Minkowski Konstante, enthält.

Auf der anderen Seite ist jedes Ideal ein Produkt von Maximalidealen. Daher enthält jede Äquivalenzklasse einen Ideal $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$, wobei die $\mathfrak{p}_i$ maximal sind und $\mathsf{N}(I) < c$. Die Multiplikativität der Norm besagt, dass

$$N(\mathfrak{p}_i) < c.$$

Als solches wird die Klassgruppe von Maximalidealen (bzw. deren Äquivalenzklassen) der Norm $< c$ erzeugt. Bei der Annahme ist jedes dieser Ideale ein Hauptideal. Als solches sind diese Äquivalent zu (1). Daher ist die gesamte Gruppe die Einheitsgruppe.

(Alternativ kann man hier auch dadurch argumentieren, dass das Produkt von Hauptidealen ein Hauptideal ist.) □

Aufgabe 12 (2 Punkte). Sei $K = \mathbb{Q}(\sqrt{11})$. Zerlege die Ideale $(2), (3)$ und (5) in Maximalideale. Beweise, dass jedes der Maximalideal die in der Zerlegung von $(2), (3)$ und (5) vorkommen Hauptideale sind. Schlussfolgere, dass $\mathrm{Cl}(\mathfrak{o}_K) = 1$ ist.

Lösung. Wir benutzen Dedekinds Primfaktorzerlegungssatz. Um $(2) \subseteq \mathfrak{o}_K$ (bzw. $(3) \subseteq \mathfrak{o}_K$) zu zerlegen, müssen wir das Minimalpolynom von $\alpha = \sqrt{11}$ modulo 2 (bzw. 3 und 5) zerlegen. Wir haben

$$\mathfrak{m}_\alpha = x^2 - 11 \equiv x^2 - 1 \equiv (x-1)^2 \mod 2,$$
$$\mathfrak{m}_\alpha \equiv x^2 + 1 \mod 3,$$

was irreduzibel ist und

$$\mathfrak{m}_\alpha \equiv x^2 - 1 = (x-1)(x+1) \mod 5.$$

Daher gilt

$$(2) = \mathfrak{p}_2^2 = (2, \sqrt{11}+1)^2,$$
$$(3) = \mathfrak{p}_3$$

und

$$(5) = \mathfrak{p}_5\mathfrak{q}_5 = (5, \sqrt{11}-1)(5, \sqrt{11}+1).$$

Als nächstes müssen wir also beweisen, dass $\mathfrak{p}_2, \mathfrak{p}_5$ und $\mathfrak{q}_5$ Hauptideale sind. Es ist klar, dass

$$\mathsf{N}(\mathfrak{p}_2) = 2, \mathsf{N}(\mathfrak{p}_5) = 5 \quad \text{und} \quad \mathsf{N}(\mathfrak{q}_5) = 5.$$

Als solches suchen wir nach Elementen mit der Norm 2 und 5, welches unsere Ideale erzeugen. Hier erinnern wir uns an die Tatsache, dass wenn $I \subseteq J$ und $\mathsf{N}(I) = \mathsf{N}(J)$, wir $I = J$ haben. Als solches suchen wir nach Elementen der Norm 2, bzw. 5, welches in $\mathfrak{p}_2$ bzw. $\mathfrak{p}_5$ enthalten sind. Dies reicht schon aus!

Sei $x = a + b\sqrt{11} \in \mathfrak{o}_K$. Dann ist $\mathsf{N}(x) = a^2 - 11b^2$. Daher suchen wir nach Paaren $a, b \in \mathbb{Z}$, so dass $|a^2 - 11b^2| = 2$, bzw. 5.

$\mathfrak{p}_2$: Man kann schnell sehen, dass $a = 3, b = 1$ so ein Paar ist. Wir wollen nun untersuchen, ob $\mathfrak{p}_2 = (3 + \sqrt{11})$. Es gilt,

$$3 + \sqrt{11} = 2 + 1 + \sqrt{11},$$

woraus $(3 + \sqrt{11}) \subseteq \mathfrak{p}_2$ folgt. Da $\mathsf{N}(\mathfrak{p}_2) = \mathsf{N}((3 + \sqrt{11}))$ haben wir auch eine Gleichheit. Per Hand können wir auch nachrechnen, dass

$$2 = (3 + \sqrt{11})(-3 + \sqrt{11}) \qquad 1 + \sqrt{11} = (3 + \sqrt{11})(4 - \sqrt{11}),$$

was die andere Seite impliziert. Dies ist jedoch nicht mehr nötig.

$\mathfrak{p}_5$ & $\mathfrak{q}_5$: Wir suchen nach a, b, so dass

$$|a^2 - 11b^2| = 5.$$

Direkte Kandidaten dafür sind $a = 4, b = \pm 1$. Wir betrachten $(4 + \sqrt{11})$ und $(4 - \sqrt{11})$. Es gilt

$$4 + \sqrt{11} = 5 - (1 - \sqrt{11})$$

was $(4 + \sqrt{11}) \subseteq \mathfrak{p}_5 = (5, \sqrt{11} - 1)$ impliziert. Gleichheit der Norm impliziert nun Gleichheit der Ideale. (Per Hand

$$5 = (4 + \sqrt{11})(4 - \sqrt{11}), 1 - \sqrt{11} = (4 + \sqrt{11})(3 - \sqrt{11})$$

was uns die Gleichheit

$$(4 + \sqrt{11}) = \mathfrak{p}_5$$

liefert). Gleichwie liefern die Gleichungen

$$5 - (1 + \sqrt{11}) = 4 - \sqrt{11}; \quad 5 = (4 - \sqrt{11})(4 + \sqrt{11}), \; 1 + \sqrt{11} = (4 - \sqrt{11})(3 + \sqrt{11}),$$

dass

$$(4 - \sqrt{11}) = \mathfrak{q}_5 = (5, \sqrt{11} + 1).$$

(Im allgemeinen ist es nicht einfach solche Paare zu klassifizieren. Wir können aber einfache Bemerkungen direkt machen. Z. B., aus $2 = |a^2 - 11b^2|$ können wir direkt schließen, dass $a^2 \equiv b^2 \mod 2$, also $a \equiv b \mod 2$ und dass $|a^2| \equiv 2 \mod 11$, daher $a \equiv 3$ oder $8 \mod 11$. Solche Beobachtungen sind natürlich öfters nicht ausreichend, aber können einige einfache Kandidaten ergeben.)

Nun geht es, die Klassgruppe zu bestimmen. Da

$$\det \begin{pmatrix} 1 & \sqrt{11} \\ 1 & -\sqrt{11} \end{pmatrix} = -2\sqrt{11}$$

und $s = 0$, haben wir

$$c = \sqrt{\Delta(\mathfrak{o}_K)} < 7.$$

Als solches kann jede Klasse von Idealen mit einem Ideal der Norm ≤ 6 repräsentiert werden. Wie schon in der vorigen Aufgabe argumentiert, reicht es aus, wenn wir uns Maximalideale der Norm $\leq c$ ansehen. Diese sind aber alle Hauptideale (wie wir es eben gezeigt haben), was $\mathrm{Cl}(\mathfrak{o}_K) = 1$ ergibt. □

Aufgabe 13 (3 Punkte). Sei $K = \mathbb{Q}(\sqrt[3]{5})$. Man darf annehmen, dass $\mathfrak{o}_K = \mathbb{Z}[\sqrt[3]{5}]$ die verstärkte Minkowski Konstante

$$c = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta(\mathfrak{o}_K)|},$$

wobei n der Grad der Erweiterung ist.

i) (1 Teilpunkt) Faktorisiere die Ideale $(2), (3)$ und (5).

ii) (2 Teilpunkte) Beweise, dass alle Maximalideale die in der Faktorisierung von $(2), (3)$ und (5) vorkommen Hauptideale sind und schlussfolgere, dass $\mathrm{Cl}(\mathfrak{o}_K) = 1$ ist.

Lösung. Als aller erstes werden wir folgendes Lemma beweisen, was unsere Argumente vereinfachen wird. (Dieses Lemma wird auch in der Vorlesungs PDF nachgetragen).

Lemma 2.0.1. *Sei $(p) = \mathfrak{pq}$, so dass $\mathfrak{p}$ ein Hauptideal ist. Dann ist auch $\mathfrak{q}$ ein Hauptideal.*

Beweis. Für ein Ideal $I \subseteq \mathfrak{o}_k$, bezeichnen wir mit $\overline{I}$ die Äquivalenzklasse in $\mathrm{Cl}(\mathfrak{o}_K)$. Da $(p) = \mathfrak{pq}$, wissen wir, dass $\overline{\mathfrak{pq}}$, die Einheit in $\mathrm{Cl}(\mathfrak{o}_k)$ definiert. Wenn also $\mathfrak{p}$ ein Hauptideal ist, dann ist $\overline{\mathfrak{p}}$ auch die Einheit von $\mathrm{Cl}(\mathfrak{o}_K)$. Da $\mathrm{Cl}(\mathfrak{o}_K)$ eine Gruppe ist, muss $\overline{\mathfrak{q}}$ auch äquivalent zu (1) in $\mathrm{Cl}(\mathfrak{o}_K) = \mathcal{I}_K^*/\mathcal{P}_K^*$ sein. (Denn in einer Gruppe folgt aus $x1 = 1$, dass $x = 1$.) Da aber in einem Quotient von Gruppen G/H, $x \sim 1 \Leftrightarrow x \in H$, muss $\mathfrak{q} \in \mathcal{P}_K^*$ sein. Daher, es muss selber ein Hauptbruchideal sein. Aber ein Hauptbruchideal, welches ein Ideal ist, ist ein Hauptideal. □

Das Minimalpolynom von $\alpha = \sqrt[3]{5}$ ist $\mathfrak{m}_\alpha = x^3 - 5$. Um dies modulo $2, 3$ und 5 zu faktorisieren setzen wir $-2, -1, 0, 1, 2$ ein und sehen, ob wir vielfache von $2, 3$ oder 5 erhalten. Es gilt

x	$x^3 - 5$
-2	-13
-1	$-6 = -2 \cdot 3$
0	-5
1	$-4 = -2^2$
2	3

was folgendes besagt:

mod 2: Das einzige Faktor ist $x + 1$ modulo 2. Daher ist $x^3 - 5 \equiv (x+1)^3$ oder $(x+1)f(x)$, wobei $f(x)$ eine irreduzible Gleichung vom Grad 2 ist. Wir haben

$$x^3 - 5 \equiv x^3 + 1 = (x+1)(x^2 + x + 1) \mod 2,$$

wobei $x^2 + x + 1$ irreduzibel ist. Dies gibt uns

$$(2) = \mathfrak{p}_2\mathfrak{q}_2 = (2, \alpha + 1)(2, \alpha^2 + \alpha + 1).$$

mod 3: Das einzige Faktor ist $x + 1$ modulo 3. Daher ist $x^3 - 5 \equiv (x+1)^3$ oder $(x+1)f(x)$, wobei $f(x)$ eine irreduzible Gleichung vom Grad 2 ist. Es gilt

$$x^3 - 5 \equiv (x+1)(x^2 - x + 1) \mod 3,$$

mit $x^2 - x + 1$ irreduzibel über $\mathbb{Z}/3\mathbb{Z}$. Dies gibt uns

$$(3) = \mathfrak{p}_3\mathfrak{q}_3 = (3, \alpha + 1)(3, \alpha^2 - \alpha + 1)$$

laut Dedekind.

mod 5: Hier ist es klar, dass

$$(5) = \mathfrak{p}_5^3 = (5, \alpha)^3.$$

Nun geht es darum zu beweisen, dass diese Maximalideale von einem einzigen Element erzeugt werden.

$\mathfrak{p}_2$, $\mathfrak{q}_2$: Wir haben $\mathsf{N}(\mathfrak{p}_2) = 2$ und $\mathsf{N}(\mathfrak{q}_2) = 4$. Daher suchen wir nach Elementen der Norm 2 und 4. Wir haben

$$\mathsf{N}(1 + \alpha) = 6 \quad \text{und} \quad \mathsf{N}(2 - \alpha) = 3,$$

was uns

$$\mathsf{N}\left(\frac{1+\alpha}{2-\alpha}\right) = 2$$

liefert. Daher suchen wir nach a, b, c mit

$$1 + \alpha = (2 - \alpha)(a + b\alpha + c\alpha^2),$$

was uns

$$\frac{1+\alpha}{2-\alpha} = 3 + 2\alpha + \alpha^2$$

liefert. Von

$$(3+2\alpha+\alpha^2) = \alpha(\alpha+1)+(\alpha+1)+2$$

wissen wir, dass $(3+2\alpha+\alpha^2) \subseteq (2,\alpha+1)$. Die Gleichheit der Norm besagt nun, dass die Ideale auch übereinstimmen. (Eine direkte Rechnung ist:

$$2 = (3+2\alpha+\alpha^2)(-1-\alpha+\alpha^2), \quad 1+\alpha = (2-\alpha)(3+2\alpha+\alpha^2)$$

wissen wir, dass $\mathfrak{p}_2 = (2,\alpha+1) = (3+2\alpha+\alpha^2)$).

Das Lemma impliziert nun, dass auch $\mathfrak{q}_2$ ein Hauptideal ist.

$\mathfrak{p}_3$, $\mathfrak{q}_3$: Wir haben $\mathsf{N}(\mathfrak{p}_3) = 3$ und $\mathsf{N}(\mathfrak{q}_3) = 9$. Da $\mathsf{N}(2-\alpha) = 3$ und $(2-\alpha) \subseteq (3,\alpha+1)$ sind die Ideale also gleich.

Vom Lemma wissen wir auch, dass $\mathfrak{q}_3$ ein Hauptideal sein muss.

$\mathfrak{p}_5$: Es ist $\mathfrak{p}_5 = (5,\alpha) = (\alpha)$, da $5 = \alpha^3$. Daher ist es ein Hauptideal.

Die Minkowski Konstante die wir hier benutzen ist

$$c = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta(\mathfrak{o}_K)|} = \frac{2\cdot 3}{3^3}\sqrt{|\mathsf{N}(\mathfrak{m}'_\alpha(\alpha))|} = \frac{2}{9}\sqrt{\mathsf{N}(3\alpha^2)} = \frac{2}{9}\sqrt{27\cdot 25} \approx 5,77.$$

Da alle Maximalideale mit Norm ≤ 5 Hauptideale sind, werden alle Ideale Hauptideale sein. □

Aufgabe 14 (2 Punkte). Sei $K = \mathbb{Q}(\sqrt{-10})$. Was ist $\mathrm{Cl}(\mathfrak{o}_K)$?

Lösung. Wir haben $\det\begin{pmatrix} 1 & \sqrt{-10} \\ 1 & -\sqrt{-10}\end{pmatrix} = -2\sqrt{-10}$ und $s = 1$, was uns

$$\left(\frac{2}{\pi}\right)^s \sqrt{\Delta(\mathfrak{o}_K)} < 4$$

liefert. Wir haben

$$x^2 + 10 \equiv x^2 \mod 2$$

was uns

$$(2) = \mathfrak{p}_2^2 = (2,\sqrt{-10})^2$$

liefert. Es gilt auch

$$x^2 + 10 \equiv x^2 + 1 \mod 3.$$

Da x^2+1 irreduzibel ist über $\mathbb{Z}/3\mathbb{Z}$, ist (3) selber ein Maximalideal. Daher ist die Klassgruppe entweder die triviale Gruppe, oder die Gruppe mit 2 Elementen. Es bleibt also zu untersuchen, ob $\mathfrak{p}_2$ ein Hauptideal ist.

Sei $x \in \mathfrak{o}_K \simeq \mathbb{Z}[\sqrt{-10}]$. Dann ist $x = a + b\sqrt{-10}$ mit Norm $\mathsf{N}(x) = a^2 + 10b^2$. Es ist klar, dass

$$a^2 + 10b^2 = 2$$

keine Lösung über $\mathbb{Z}$ hat, woraus wir schließen können, dass $\mathfrak{p}_2$ kein Hauptideal ist. □

Aufgabe 15 (1 Punkt). Sei K ein Zahlenkörper und $p \in \mathbb{Z}$ eine Primzahl, so dass $p \nmid \mathrm{Cl}(\mathfrak{o}_K)$. (Also, p teilt die Klassgruppe nicht).

Sei I ein Ideal von $\mathfrak{o}_K$, so dass $I^p = (\theta)$ ein Hauptideal ist. Beweise, dass I ein Hauptideal ist.

Lösung. Dies folgt vom Satz von Lagrange, welches besagt, dass die Ordnung eines Elements, die Ordnung der Gruppe Teilt. - Also, wenn G eine endliche Gruppe von Ordnung n ist (also n Elemente hat) und $g \in G$ ein Element von Ordnung m ist (also, $g^m = 1$ und aus $g^i = 1$ folgt $i = 0$ oder $i \geq m$), dann gilt $m \mid n$.

Sei nun $G = \mathrm{Cl}(\mathfrak{o}_K)$ unsere Klassgruppe und $g = \overline{I}$ die Äquivalenzklasse von I. Bei Annahme ist $I^p = (\theta)$ ein Hauptideal, daher $g^p = 1$ in der Klassgruppe. Da p eine Primzahl ist, muss die

Ordnung von g entweder 1 oder p sein. (Wenn es nicht klar ist, sollte man es selber versuchen zu begründen).

Wenn aber die Ordnung von g die Primzahl p wäre, so müsste p die Ordnung von $G = \mathrm{Cl}(\mathfrak{o}_K)$ teilen. Bei Annahme tut es dies jedoch nicht. Daher muss die Ordnung von g also 1 sein, was $g = 1$ impliziert. - Also ist I ein Hauptideal. □

Aufgabe 16 (4 Punkte). Sei $K = \mathbb{Q}(\sqrt{-14})$.

i) [1 Teilpunkt] Beweise, dass jede Äquivalenzklasse von Idealen (unter der Äquivalenz $\mathrm{Cl} = \mathcal{I}_K^*/\mathcal{P}_K^*$) einen Ideal der Norm ≤ 4 enthält.

ii) [1 Teilpunkt] Zeige, dass $(2) = \mathfrak{p}_2^2 = (2, \sqrt{-14})^2$ und $(3) = \mathfrak{p}_3\mathfrak{q}_3 = (3, 1+\sqrt{-14})(3, 1-\sqrt{-14})$.

iii) [1 Teilpunkt] Beweise, dass $(2-\sqrt{-14}) = \mathfrak{p}_2\mathfrak{p}_3^2$.

iv) [1 Teilpunkt] Schlussfolgere, dass $\mathrm{Cl}(\mathfrak{o}_K)$ die zyklische Gruppe mit 4 Elementen ist.

Lösung. i) Wir haben

$$\det\begin{pmatrix} 1 & \sqrt{-14} \\ 1 & -\sqrt{-14} \end{pmatrix} = -2\sqrt{-14}$$

und $s = 1$, was uns

$$\left(\frac{2}{\pi}\right)^s \sqrt{\Delta(\mathfrak{o}_K)} < 5$$

gibt. Daher enthält jede Äquivalenzklasse von Idealen in $\mathrm{Cl}(\mathfrak{o}_K)$ einen Ideal der Norm ≤ 4.

ii) Es gilt $\mathfrak{m}_\alpha = x^2 + 14 \equiv x^2 \mod 2$ und $\mathfrak{m}_\alpha \equiv x^2 - 1 = (x-1)(x+1) \mod 3$, was uns

$$(2) = \mathfrak{p}_2^2 = (2, \sqrt{-14})^2$$

und

$$(3) = \mathfrak{p}_3\mathfrak{q}_3 = (3, \sqrt{-14}-1)(3, \sqrt{-14}+1)$$

gibt.

iii) Sei $a = 2 - \sqrt{-14}$. Es ist klar, dass $a \in \mathfrak{p}_2$ und $a \in \mathfrak{p}_3$. Als solches gilt $\mathfrak{p}_2 \mid (a)$ und $\mathfrak{p}3 \mid (a)$. Da $\mathfrak{p}_2 \neq \mathfrak{p}_3$ (Normen sind verschieden) und beide Maximal sind, folgt, dass $\mathfrak{p}_2\mathfrak{p}_3 \mid (a)$. Daher gibt es ein $\mathfrak{x} \subseteq \mathfrak{o}_K$, so dass

$$(2-\sqrt{-14}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{x}.$$

Wir haben $\mathsf{N}((a)) = |4+14| = 18$. Daher muss $\mathsf{N}(\mathfrak{x}) = 3$ gelten, woraus $\mathfrak{x} = \mathfrak{p}_3$ oder $\mathfrak{x} = \mathfrak{q}_3$ folgt, da diese die einzigen Ideale mit Norm 3 sind.

Wenn $\mathfrak{x} = \mathfrak{q}_3$, dann $(a) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{q}_3 = \mathfrak{p}_2(3)$, woraus $(3) \mid (a)$, also $a \in (3)$ folgt. Dies ist offensichtlich ein Widerspruch. Daher muss $\mathfrak{x} = \mathfrak{p}_3$ sein. Also,

$$(a) = \mathfrak{p}_2\mathfrak{p}_3^2.$$

iv) Wir wissen, dass die einzigen Elemente von $\mathrm{Cl}(\mathfrak{o}_K)$ die Äquivalenzklassen von $(1), \mathfrak{p}_2, \mathfrak{p}_3$ und $\mathfrak{q}_3$ sein kann. Als erstes bemerken wir, dass kein Element in $\mathfrak{o}_K$ die Norm 2 oder 3 hat. Daher sind $\mathfrak{p}_2, \mathfrak{p}_3$ und $\mathfrak{q}_3$ alle unterschiedlich von (1). Daher kann $\mathrm{Cl}(\mathfrak{o}_K)$ nur eines der folgenden Gruppen sein: $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z}$.

Da jedoch $(a) = \mathfrak{p}_2\mathfrak{p}_3^2$ gilt

$$(1) \simeq \overline{\mathfrak{p}_2\mathfrak{p}_3}^2,$$

wobei $\overline{\mathfrak{p}_i}$ die Äquivalenzklasse des Ideals in $\mathrm{Cl}(\mathfrak{o}_K)$ bezeichnet. Da $\mathfrak{p}_2^2 = (2)$ haben wir

$$\overline{\mathfrak{p}_2}^2 \simeq (1)$$

in $\mathrm{Cl}(\mathfrak{o}_K)$ was zusammen mit der obigen Gleichung

$$\overline{\mathfrak{p}_2} \simeq \overline{\mathfrak{p}_3}^2$$

ergibt. Da $\overline{\mathfrak{p}_2}$ ja Ordnung 2 hat (Quadrat davon ist die Einheit, ist aber selber nicht die Einheit), muss $\overline{\mathfrak{p}_3}$ Ordnung 4 haben. Daher muss die Gruppe $\mathbb{Z}/4\mathbb{Z}$ sein, da es die einzige Gruppe mit 4 Elemente ist, die ein Element der Ordnung 4 hat.

□